Secure QoS-Aware Data Fusion to Prevent Node Misbehavior in Wireless Sensor Networks

Shaila K*, Nalini L*, Tejaswi V*, Thriveni J*, Venugopal K R*, L M Patnaik**

*Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001, India.
**Vice Chancellor, Defence Institute of Advanced Technology, Pune, India

Abstract
Wireless Sensor Networks(WSNs) are composed of tiny devices with limited computation and energy capacities. Data fusion is an essential technique to achieve power efficiency in sensor nodes. Some nodes misbehave by increasing the defer time which obstruct the data fusion process. In this paper, an efficient Secured Quality of Service(QoS)-Aware Data Fusion(SQDF) for distributed Wireless Sensor Networks is proposed. The key feature of secure data fusion is to detect the misbehavior of a node which defers the data packet for an extra period of time. Simulation results show that proposed scheme efficiently detects the malicious nodes and decreases the packet drop significantly.

Key words:
data fusion; data transmission; energy; malicious nodes; power efficiency; Quality of Service.

1. Introduction

Recent development in the manufacturing of electronic components such as microprocessors, memory chips and development in the field of wireless networking have led to the development of WSNs. The collection of large number of low cost sensor nodes having sensors, processors, memory chips and wireless transceivers are deployed in a network. Sensor network is used in many applications such as military, agriculture, detection of forest fire, nuclear attacks and health. WSNs should be robust, since such networks can be efficiently used in real time application.

Data fusion is a process of aggregating certain combination of packets without losing any important data. Data fusion is performed in a distributed fashion based on the available local information. It can be performed at the intermediate nodes as well as at the end nodes. Data can be fused at the intermediate nodes to satisfy end-to-end delay constraint whereas at the end nodes it is performed to balance the delay and buffer overflow.

Security in WSNs has six challenges. They are : *(i* Wireless nature of communication *(ii)* Resource limitation in sensor nodes *(iii)* Deployment of sensor nodes *(iv)* Lack of fixed infrastructure *(v)* Unknown network topology prior to deployment *(vi)* High risk of physical attacks to unattended sensors. Wireless communication helps malicious nodes to perform variety of active and passive attacks. In active mode of attack, malicious nodes actively interrupt the system by capturing or reading the contents of the sensor nodes. They either insert, modify or delete the data so as to jam a part of or the whole network. In passive mode of attack, malicious nodes silently listen to the channel to capture the data or security information illegally and thus it provides enough information about the hostile nodes. For example malicious nodes can initiate active attacks by increasing the value of the delay constraint used in data fusion technique and reduce the probability of successful packet delivery.

Wireless networks are more vulnerable to attacks than wired networks because of the broadcast nature of transmission medium and resource limitation. Some of the security requirements in WSNs are: *(i) Availability* : Whenever an application requires service, the complete network or atleast a single sensor node should take the responsibility of providing the service. *(ii) Authentication* : In order to share the secret information, a node should be authenticated by other nodes or control center. *(iii) Integrity* : The message should not be altered by malicious nodes. *(iv) Confidentiality* : Providing privacy to wireless channels to prevent eavesdropping. *(v) Non-reputation* : The nodes are monitored so that malicious nodes cannot hide their activities. In addition to these general requirements, WSNs has some specific requirements like *(a) Survivability* : Providing minimum level of service in case of power loss or attacks. (*b) Degradation of security services* : As the resource availability to the sensor nodes change, security level should be varied.

In the recent years WSNs have found their way into a wide variety of applications and systems with varying requirements and characteristics. The classification of applications is based on the design space, deployment, mobility, resources, lifetime, QoS, connectivity, coverage, topology and infrastructure. WSNs are used in

Manuscript received March 5, 2011
Manuscript revised March 20, 2011

industry, public safety, automobile, hazardous chemical levels and fires, commercial sector, medical field and electrical sector.

Motivation : Data fusion can be used to decrease the traffic load and energy consumption thus increasing the network lifetime. Data fusion is performed by specifying the delay constraint within which data is collected at the intermediate nodes and fusion is performed. This inturn increases the packet drop. Some nodes increase the delay constraint maliciously and further increase the packet drop. So, there is a necessity to propose a solution to determine the malicious nodes efficiently and thus reduce the packet drop.

Contribution : In the proposed secured data fusion technique, data fusion is performed with reliability. Some malicious nodes are introduced in the network which defers the packet for extra period than the actual specified time. Node's with malicious nature increases the packet drop. To overcome this problem, neighboring nodes of a particular node monitors the node and if it finds the stated misbehavior then that node is excluded from the network. Hence, the network is secured with reduced packet drop. It should be noted that packet drop in secured data fusion technique is nearly equal to the data fusion technique that is not secured. Thus, the proposed scheme efficiently provides the security to the network.

Organization : In Section 2, research works in the data fusion techniques and security issues are discussed. Problem definition is stated in Section 3 and Data Fusion Technique is explained in Section 4. Algorithm to provide a security to Data Fusion Technique called SQDF is proposed in Section 5. Implementation details are explained in Section 6. Simulation details are illustrated in Section 7 and Conclusions in Section 8.

2. Related Work

Tian et al., [1] proposed the concept to determine the effect of measurement and communication errors on the tradeoff in the design of clustered sensor networks. In clustered multihop sensor network, sensor nodes use their observations of the environment to take decisions about whether an event has occurred. Each node transfers this decision to the control center. Optimal decisions at the control center is obtained by thresholding a weighted sum of node's local decisions. The optimal weights are considered as a function of bit error probability of channel and ring from which the decision is originated.

Jin et al., [2] presents a QoS-Constrained DAta fusion and Processing (QDAP) for Wireless Sensor Networks. In the paper, QoS requirements are taken into account to determine when and where to perform fusion. Data fusion is performed at the intermediate nodes and also end-to-end constraint is satisfied. To balance the design tradeoffs of delay, measurement accuracy and buffer overflow localized adaptive data collection algorithm is proposed to collect the data at the end nodes. The proposed idea is evaluated on different matrices such as energy efficiency, network life time, end-to-end latency and data loss.

Tara et al., [3] explain about the intermittent-connectivity network. It is a network in which connected path between source and destination exists very rarely because of limited transmission range. A node generates and stores the data and on reaching the communication range of another node it replicates the data. Multiple copies of the packet decrease the time to offload data to the destination, but increases energy and storage used in the system. Resource-delay tradeoff and capacity of intermittent connectivity with QoS restrictions such as communication bandwidth is quantified.

Hong et al., [4] propose a protocol called Reliable Data Aggregation which associates packet's reliability in data transmission with the amount of information it contains and gives higher reliability to the packet which has more information. The reliable data aggregation can jointly optimize both information reliability and energy efficiency in sensor networks with data fusion.

Bhaskar et al., [5] compare the traditional end-to-end routing scheme and data-centric routing scheme. Data-centric is a mechanism that performs in-network aggregation of data needed for energy efficient information flow. The impact of source destination placement and communication network density on the energy costs and delay associated with data fusion is presented. It is shown that data-centric routing offers significant performance gains across a wide range of operational scenarios over traditional end-to-end routing scheme. Information about the location of control center is continuously propagated throughout the sensor field to keep all sensor nodes updated with data reports. This leads to both excessive drain of sensor's limited battery power and increased collisions in wireless transmissions.

Fan et al., [6] describe Two-Tier Data Dissemination that provides scalable and efficient data delivery to multiple mobile sinks. Node compromise leads to severe security threats in Wireless Sensor Networks and the security protection breaks down when threshold is exceeds. Hao et al., [7] discuss an idea to overcome the threshold limitation and achieve resiliency against node compromise. Location-based approach is proposed in which the secret keys are bound to geographic locations and each node stores few keys based on its own location. The location-binding property constraints the scope for which individual keys can be used, thus limiting the damages caused by a collection of compromised nodes.

Jing et al., [8] considers routing security. This paper deals with the attacks against sink holes and hello floods in sensor networks. They describe the clipping attacks and suggest the countermeasures. Multipath routing to multiple control centers is analyzed to provide tolerance against individual control center attacks and disguise the location of control center from eavesdroppers, explains relocation of control center in case of damage and enhances resiliency of the network.

Maarten Ditzel et al., [9] present the result of a study on the effects of data fusion for multi-target in WSNs. Normally WSNs has limited bandwidth and nodes with limited computing power and limited battery life. The main aim is to accurately track multiple targets crossing an area observed by Wireless Sensor Networks, while limiting the amount of network traffic. Various computing power aware data aggregation strategies are presented which helps in reducing energy consumption and tracking accuracy.

Hop-by-hop data fusion is a very important technique for reducing the communication overhead and energy consumption of sensor nodes during the process of data collection in a sensor network. Individual sensor readings are lost in the per-hop fusion process, compromised nodes in the network may forge false values as the fusion result of other nodes. To avoid such problems Secure Hop-by-Hop Data Aggregation Protocol [10] is proposed. The design of this protocol is based on the principles of *divide-and-conquer* and *commit-and-attest*. The nodes in a tree are partitioned into multiple logical groups of similar sizes and commitment-based hop-by-hop fusion is performed in each group to generate a group aggregate. The control center identifies the suspicious groups based on the set of group aggregate.

Przydatek et al., [11] proposed a novel frame work for secure information aggregation in large sensor networks. Certain nodes in a network, called *aggregators*, help in aggregating information requested by query, which reduces the communication overhead. By constructing efficient random sampling mechanisms and interactive proofs, it is possible for a user to verify the answer given by the aggregator which is the good approximation of a true value when aggregator and a fraction of the sensor nodes are corrupted.

Lageweg et al., [12] compare the fusion strategies for multi-target tracking. The effect of noise(considered as false contacts) on the accuracy is verified. Central track algorithm is proposed to associate the individual measurements with tracker and estimates the target's position and velocity. The tracker can ideally separate true targets from false contacts.

Intanagonwiwat et al., [13] proposed a Directed Diffusion. The basic idea of this protocol is to construct data fusion tree which collects the data at the control center where it is rooted. When data is delivered from any node to control center, aggregation occurs at the control center without interacting with the node to eliminate redundancy and to reduce transmission energy. They have mainly concentrated on energy aspect of data aggregation and have considered reliability.

Younis et al., [14] proposed the autonomous WSNs as a service platform whose mission is to provide dependable information to satisfy QoS requirements. A new scheme safety-aware relocation pursues relocation of the aggregation and forwarding nodes to boost the network performance without compromising the safety of the aggregation and forwarding nodes.

Carlos et al., [15] have done a survey on Wireless Sensor Networks, their technologies, standards and applications. Many routing, power management and data dissemination protocols with energy awareness as an important design issue are discussed. James et al., [16] measure the quality of spatial resolution. In a network all the sensors participate equally in the network at the same time it conserves the energy and maintains the desired spatial resolution. The parameters such as mean and variance of the QoS are taken into consideration to control the network performance.

Barton et al., [17] explain the traffic patterns in Wireless Sensor Networks as many-to-one or one-to-many communication. Performance can be characterized by the rate at which data can be fused at the collector center. The fusion rate of $\theta[(\log n)/n]$ is optimal and it can be achieved using time-reversal communication. Jie Gao et al., [18] formulated the problem of performing the data aggregation for sparse nodes. When the sensors are deployed to detect relatively rare events, each node which participates in the fusion must be queried. Instead of blindly querying all the nodes in the network, it is feasible to discover the interesting nodes to get statistical summaries. The key idea is the capability for two nodes that wish to communicate at the same time to discover each other at a cost that is proportional to the network distance.

Hartley et al., [19] discussed the problem of inferring per node loss rates from passive end-to-end measurements in Wireless Sensor Networks. They have shown how to adapt network interference, so that loss rates in WSNs are inferred. This includes per node loss rates and considering the unique characteristics of Wireless Sensor Networks. The problem of Maximum-Likelihood Estimation is solved using Expectation-Maximization. The result of inference procedure can be used to stream-line the data collection process.

3. Problem Definition

In a Wireless Sensor Networks consisting of *N* nodes, if there exists *x* malicious nodes in the same network, then the packet delivery ratio is decreased. Security must be provided to the network against such malicious nature so that packet drop is decreased.

Objective : The main objective of the proposed concept is to perform data fusion process at the intermediate nodes to decrease the traffic load, reduce energy consumption and obtain reliability.

Assumptions : To implement Secured QoS-Aware Data Fusion, the following conditions are assumed for the WSNs.

(i) All nodes defer the packet for same period of time before data fusion process.
(ii) Packet origination rate at all the nodes follows an exponential distribution.
(iii) Control Center cannot be a malicious node.
(iv) Routing paths are predetermined and the routes from individual node to the control center is identified by the edges between various nodes and is modified only when a malicious node is detected in the network.
(v) The transmitting range of each node is assumed to be 50 meters.

4. Data Fusion Techniques

Data fusion can be performed at two levels in a network.
(i) Collecting the data packets at the end nodes.
(ii) Fused data is transmitted from end nodes to the control center through intermediate nodes.

At the end nodes, multiple samples are collected and fused together into a single packet for energy efficiency purpose and when an intermediate node receives a packet, forwards the packet or performs local processing. To achieve QoS constraints it is necessary that intermediate nodes perform data fusion process before forwarding a packet.

To perform data fusion at intermediate nodes, each node defers for a particular time for collecting set of packets over a period of time. Those packets can be used for data fusion process in order to decrease network load and energy efficiency. Under such scenarios, malicious nodes defer for extra period of time than expected. Due to such malicious nature of a node, the following situations arises;

(i) Decrease in the successful packet delivery to the control center from the sensor nodes.
(ii) Threat to lose some important information because of extra deferred time.
(iii) End-to-end delay increases which drastically decreases the network lifetime.

So, there is a necessity that the simulation should identify such malicious nodes and exclude them from the network topology, *i.e.,* no packets should be forwarded to such malicious nodes and descendents of those nodes should be connected to the nearest well-behaving node for the continued network operation.

5. Algorithms

Every node in a network defers the packet for a certain period of time for data fusion process. In a network there may be one or more malicious nodes, which reduces the network throughput. A malicious node considered is called *delay hole*. Delay hole defers the packet for extra time than the specified time. As a result of this, most of the packets will be dropped because their exists an end-to-end delay constraint which increases the packet drop. Increase in number of such malicious node lead to network failure.

In order to avoid network failure, it is necessary to find a solution which announces a new routing scheme to exclude the malicious nodes from the network. To achieve this, an algorithm for Secured QoS-Aware Data Fusion process with the routing scheme is proposed in this paper. Algorithm effectively detects the malicious node, advertises this information to the network and new routing information are announced. Algorithm consists of four phases in order to find a malicious node.

In the first phase each node broadcasts the *hello messages* in the network to determine it's neighbors and also to know the average transmission time required to transfer the packet between any two nodes.

In the second phase, when a packet is received by a node, it defers the packet for certain time which is required for data fusion process and sends the packet to its parent node. This packet is received by the source node which checks the behavior of a node. A node defers the packet for extra time over many transmissions, then the node is considered to be a malicious node. This observation is communicated throughout the network in the third phase by broadcasting report message which finally reaches the control center.

Control center receives the report from different nodes. Upon receiving this report, control center broadcasts the decision message to the network and also

Algorithm : Secure QoS-Aware Data Fusion (SQDF)

```
First Phase
 begin
    Broadcast Hello Message
    Determine average transmission time
    Send Data Packet
 end

Second Phase
 begin
     Receive Data Packet
     if(malicious node)
     Reset the timer for (defer time + extra time)
     else
     Reset the timer for defer time
     Fuses data till timer expires
     if (timer expires)
     Send Data Packet
 end

Third Phase
  begin
     Check parent node's behavior
     if (parent node is malicious)
     Broadcast Report Message
     else
     Send Data Packet
  end

Fourth Phase
  begin
      Receive Report Message
      Find new routing path excluding malicious node
      Broadcast Decision Message
  end
```

communicates the new routing information.

Initially each node called *source node* broadcasts the *hello message* which includes the time stamp at which the packet has been sent. All the neighboring nodes receive this message and sends an acknowledgment by including the current time stamp in the message. Source node receives this message and finds the transmission time required to transfer the packet from source node to the node which has sent an acknowledgment. After transferring n such packet between any two nodes, average transmission time is calculated.

Average transmission time is determined by considering n such data transfers. The motivation for considering n such data transfer is that, a node may not find out the exact transmission time because of channel error, interference, traffic load, *etc.,* and legitimate nodes may be accused as malicious for deferring the packet for extra time. Average transmission time(T) when the n packets are sent by, say, the first node is,

$$T_{1i} = [(t_{11} + t_{12} + t_{13} + \ldots + t_{1n}) / n]$$

second node is,

$$T_{2i} = [(t_{21} + t_{22} + t_{23} + \ldots + t_{2n}) / n]$$

In general for N nodes' surrounding a particular node is,

$$T_{Ni} = \sum_{N=1}^{m} \sum_{i=1}^{n} \frac{t_{Ni}}{n}$$

After calculating the average transmission time, during data transfer when a node receives the data packet from the leaf node, it defers the packet for t time, assigns the current time and forwards the packet to its parent node. Since, the data transfer takes place through omni-directional antenna, source node receives this packet and checks whether the intermediate node is malicious or not. In order to find out the defer time, source node considers the packet origination time and the time at which the source node receives it from its parent. The difference gives the d_{time}.

A node is said to be behaving according to the protocol specification if the defer time d_{time} is

$$d_{time} \leq 2(T) + t$$

If d_{time} is greater than the time required for transmission and defer time, then that node is considered as a malicious node. A threshold is maintained which indicates the maximum number of packets which can be deferred for time greater than d_{time}. If the threshold exceeds *i.e.,* $d_{timethres} \geq d_{time}$, then a node is accused as a *delay hole* and the source node broadcasts the report message into the network which finally reaches the control center.

In the final phase, control center receives the report message about a particular node as delay hole. If majority of nodes send the report that a node is delay hole then control center declares the node as malicious node and broadcasts this decision message to the network. Malicious node is determined when all the neighboring nodes decides that it is a *delay hole* by observing the transmission time taken for the transmitting n packet by m nodes. Thus, a node is malicious when,

$$\text{malicious node} = \sum_{i=1}^{n} T_{1i} = \sum_{i=1}^{n} T_{2i} = \sum_{i=1}^{n} T_{3i} = \cdots = \sum_{i=1}^{n} T_{mi}$$

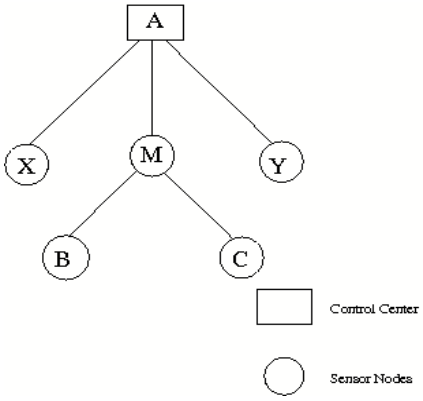


Fig.1 Original Topology

Control center is a central authority which has the routing information of all the nodes which has to exclude the malicious node from the network and specify the new routing scheme. Control center verifies its routing information to determine the descendents of the malicious node and finds the nearest non-malicious node. It directs the descendents of a malicious node to get connected to the non-malicious node. This process continues and if there are any such malicious nodes in the network, they are excluded from the network. The proposed algorithm efficiently detects the misbehaving node at the same time successful packet delivery probability can be increased.

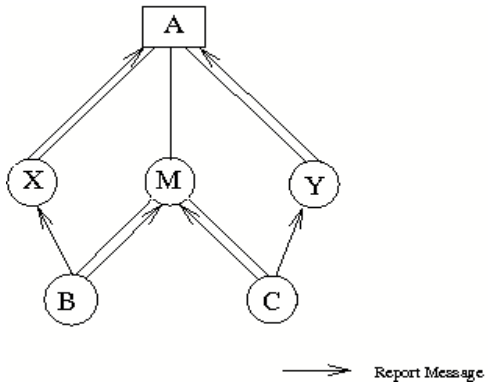


Fig. 2 Report message indicating M as malicious

The implementation is summarized in the algorithm. The first phase is executed by every node in the network. Second phase of the algorithm is executed upon receiving the data packet by an intermediate node. Once a node gets to know about its parent it executes the third phase of the algorithm and finally a control center executes the fourth phase.

For instance, consider a topology depicted in Figure 1. *A* represents the control sender which is responsible for taking major decisions such as whether the node is behaving properly and broadcasting this decision in the network. Sensor nodes are responsible for performing data fusion process and transmitting such fused data to the control center.

Figure 2 explains how the report message is broadcasted to network and finally reaches the control center. Consider a node *M* misbehaving by deferring the packet for 0.8 seconds whereas the actual defer time is 0.5 seconds with an extra defer time of 0.3 seconds. Initially, when a *hello* message is sent by node *B* and node *C* periodically to node *M*, both receive acknowledgments from node *M* and the difference in *hello* message origination time and the time at which acknowledgment is received gives the *avg_ transmit_ time*.

During data transfer process, node *M* defers the packet for extra time than actual specified time and broadcasts that packet which is received by node *B* and node *C*. Both the nodes find out the defer time as stated earlier and these nodes come to the conclusion that node *M* is misbehaving by considering many transmissions. The report of its observation is broadcasted into the network which is finally received by the control center.

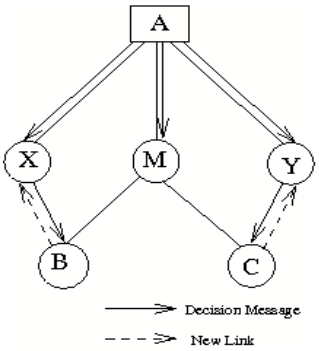


Fig. 3 Decision message by control center and establishing new links

Control center receives the reports from node *X* and node *Y* and it comes to the conclusion that node *M* is misbehaving. Now the control center broadcasts the decision saying that node *M* is misbehaving and it also instructs node *B* and node *C* to get connected to node *X* and node *Y* respectively and not with node *M*. Thus, a malicious node *M* is successfully excluded from the network as shown in Figure 3.

6. Implementation

Implementing QoS- Secured Data Fusion involves three different types of messages other than the data that has to be sent. *Hello* message is used to evaluate the average time required to send a data from a node to its parent. Every node transmit a *hello* message periodically to update the node's information at that particular instance. This message is transmitted to only one hop neighbors and average time is calculated.

A source node detects an intermediate node behaving maliciously, it broadcasts a *report* message to the control center informing about the malicious node. A *report* message consists of malicious node's information with the higher time-to-live value. *Decision* message is sent by the control center to indicate the source nodes about its new routing path to the control center.

The aggregation of data requires certain waiting time by all the intermediate nodes which increases the end-to-end delay. The restriction on end-to-end delay called *delay constraint D* is used to increase the efficiency of the network. The value of *D* emphasize on every data packet to be received within a fixed time interval. The packet is dropped when the difference between the time of receiving packet by control center and its origination time is greater than the delay constraint *D*.

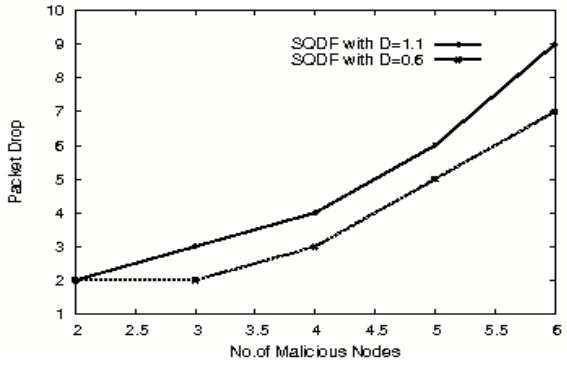


Fig. 4 Malicious Node and Packet Drop

The origination of a report message by a source node depends on the defer time by its parent. When a parent node sends data after aggregation, the source node checks the time parent has waited for aggregation. If this time is greater than the normal defer time, then the parent node is said to be misbehaving. Because of a traffic load in a network, the transmission time may vary. Hence, a threshold of twice the transmission time is considered to detect a malicious node.

Since the control center has a routing information of all the nodes, it takes a decision of a new routing path for a node from which it receives a *report* message. A new routing information is broadcasted to a node through *decision* message. For implementation purpose, a delay constraint D = 0.6 and D = 1.1 seconds and an exponentially distributed data origination rate among all the sensor nodes is considered. Exclusion of malicious nodes is implemented by nodes not sending a data packets to misbehaving nodes.

7. Simulation

In this section, the complete performance evaluation of the proposed quality-oriented, secured data fusion process in multi-hop sensor networks is accomplished by simulating using the Network Simulator(NS2). For the study of the sensor network, a random topology consisting of sensor nodes and single control center is considered. The area of node deployment for the simulation is 100*m* x 200*m*. In order to focus on the study of security with data fusion and packet delivery ratio, routing paths are assumed to be predetermined unless there is command by a control center to modify the existing topology if any malicious nodes are detected. The routes from each sensor node to control center are identified by the edges between various nodes.

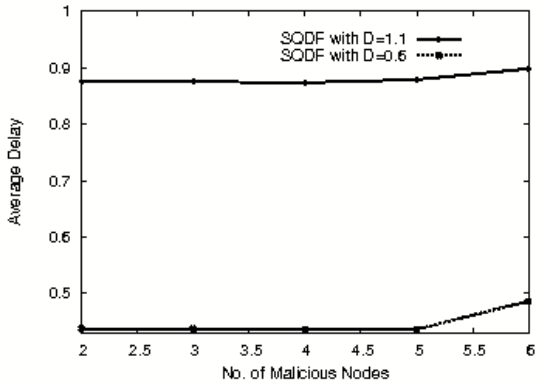


Fig. 5 Malicious Node and Average Delay

The simulation is run for 1800 seconds. Each simulation is run for different number of malicious nodes to determine how the network security is disrupted with increase in the number of malicious nodes. The simulation results are obtained for different delay constraints. The simulation is used to evaluate the effect of security in data fusion process. Significant improvement is achieved in successful packet delivery ratio and all the malicious nodes are accurately detected and is excluded from the network.

In this section, effect of number of malicious nodes on the successful packet delivery is discussed. The corresponding graph is shown in Figure 4. The graph is

plotted for delay constraint D = 0.6 and D = 1.1. From the graph, it is shown that as the number of malicious nodes increase in the network, successful packet delivery decreases. It is observed that as the number of malicious nodes increase, defer time for a particular packet by each node also increases. Most of the packets are dropped because the delay constraint D expires. It is also noted that there is considerable decrease in packet drop as the delay constraint is increased.

Average delay of a packet is the average time required to reach the control center. The average delay is observed to be less than the delay constraint D. The average delay graph is plotted with D = 0.6 and D = 1.1 in Figure 5. As the number of malicious nodes increase, the defer time for a particular packet by such malicious nodes increase which results in increased average delay.

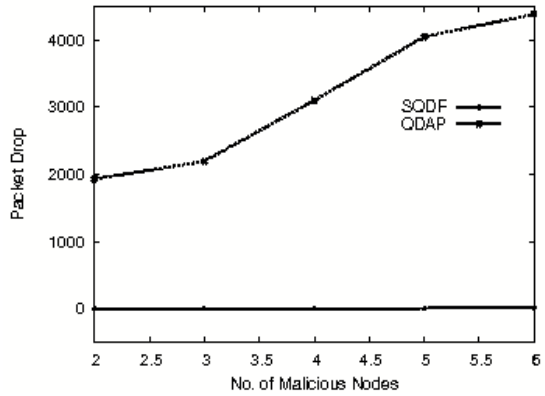


Fig. 6 QDAP Vs SQDF with D=0.6

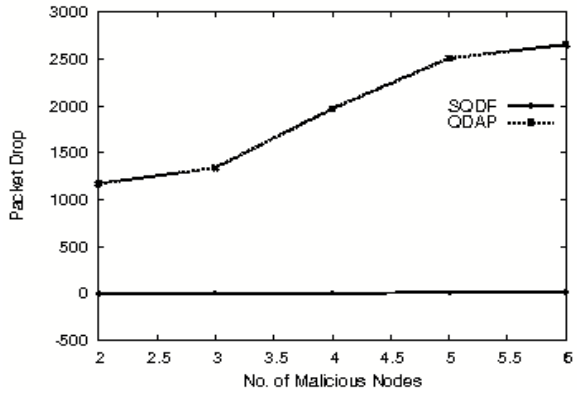


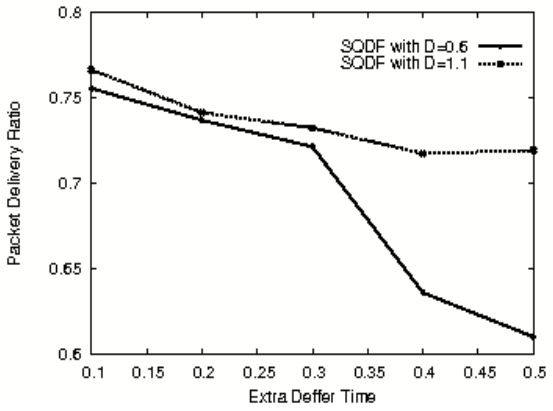
Fig. 7 QDAP Vs SQDF with D=1.1

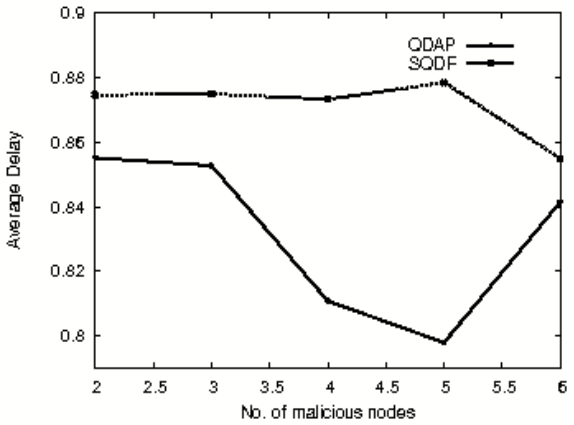
Comparison of packet drop between QoS and Secured QoS is presented in Figure 6. As the number of malicious nodes increases it leads to increased packet drop as explained previously. The comparison shows significant decrease in the packet drop when security concept is added to the network. It should be noted that packet drop in data fusion process without any malicious nodes is equal to the packet drop in Secured QoS. This indicates that security is provided to the network without dropping an extra packet. The comparison is performed for different delay constraints and corresponding graphs are plotted in Figure 6 and Figure 7.

The effect of increased packet defer time leads to increase in packet drop. As the defer time increases by a malicious node, more packets are dropped before it reaches the control center. The corresponding comparison of defer time and packet drop is plotted in Figure 8. Variation in the extra time deferred by a malicious node is between 0.1 and 0.5 seconds. It is

Fig. 8 Malicious Node and Packet Drop

Fig. 9 Malicious Node and Packet Drop





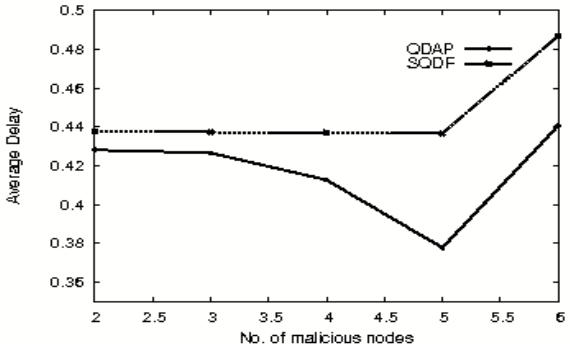


Fig. 10 Malicious Node and Packet Drop

noted that as the defer time increases, number of packets dropped is increased reducing the packet delivery ratio. Comparison of average delay with normal QoS and Secure QoS is plotted in Figure 9 and Figure 10. From the graphs it is clear that there is a negligible increase of average delay in secure QoS as compared to normal. This is the overhead involved because of addition of security to the QoS-aware data fusion. The overhead incurred can be afforded to secure system. Graphs are plotted for different delay constraints, $D = 0.6$ and $D = 1.1$.

8. Conclusions

This paper proposes an efficient Secured QoS-Aware Data Fusion and processing for Wireless Sensor Networks. The proposed approach includes the fusion of data at the intermediate nodes simultaneously providing security to the network. Secured data fusion technique reduces the packet drop which is caused by the malicious nodes at the same time reduces the traffic load and increase the network life time. To evaluate, varied number of malicious nodes under different traffic scenarios and traffic load is considered. The corresponding numerical results demonstrate the significant performance improvement interms of reduced packet drop and delay and at the same time malicious nodes are excluded from the network. This makes the network secure and reliable. Hence, it can be efficiently used in real time applications such as in military applications where sensor networks may be exposed to hostile environment. The proposed scheme is evaluated using fixed sensor networks. This approach can be combined with appropriate routing technique and thus can be used in dynamic network environment.

References

[1] Quigjiang Tian, Edward J.Coyle and Fellow, "Optimal Distributed Detection in Clustered Wireless Sensor Networks", in IEEE Transactions on Signal Processing, vol. 55, no. 7, pp. 3892-3904, July 2007.

[2] Jin Zhu, Symeon Papavassiliou and Jie Yang, "Adaptive Localized QoS-Constrained Data Aggregation and Processing in Distributed Sensor Networks", in IEEE Transactions on Parallel and Distributed Systems, vol. 17, no. 9, pp. 923-933, September 2007.

[3] Tara Small, Zygmunt J. Haas and Fello, "Quality of Service and Capacity in Constrained Intermittent Connectivity Networks", in IEEE Transactions on Mobile Computing, vol. 6, no. 7, pp. 803-814, July 2007.

[4] Hong Luo, Qi Li and Wei Guo, "RDA: Reliable Data Aggregation Protocol for Wireless Sensor Networks", in Proceedings of IEEE International Conference in Wireless Communications, Networking and Mobile Computing, pp. 1-4, September 2006.

[5] Bhaskar Krishnamachari, Deborch Estrin and Stephen Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks", in Proceedings of the Twenty Second IEEE International Conference on Distributed Computing Systems, pp. 575-578, July 2002.

[6] Fan Ye, Hui Luo, Jerry Cheng, Songwu Lu and Lixia Zhang, "A Two-Tier Dissemination Model for Large Scale Wireless Sensor Networks", in MOBICOM, pp. 148-159, September 2002.

[7] Hao Yang, Fan Ye, Yuan Yuan, Songwu Lu and William Arbaugh, "Towards Resilient Security in Wireless Sensor Networks", in Proceedings of the Sixth ACM International Symposium on Mobile AdHoc Networks and Computing, MOBIHOC, pp. 34-45, May 2005.

[8] Jing Deng, Richard Han and Shivakant Mishra, "Enhancing Base Station Security in Wireless Sensor Networks", in Department of Computer Science Technical Report, University of Colorado, pp. 1-17, April 2003.

[9] Maarten Ditzel, Caspar Lageweg, Johan Janssen and Arne Theil, "Multi-Target Data Aggregation and Tracking in Wireless Sensor Networks", in Journal of Networks, vol. 3, no. 1, pp. 1-9, January 2008.

[10] Yi Yang, Xinran Wang, Sencun Zhu and Guohong Cao, "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks", in ACM Transactions on Information and System Security, vol. 11, issue 4, 18(1:43), July 2008.

[11] Bartosz Przydatek, Dawn Song and Adrin Perrig, "SIA: Secure Information Aggregation In Sensor Networks", in Proceedings of The First International Conference on Embedded Networked Sensor Systems, pp. 255-265, November 2003.

[12] C.Lagewueg, J. Janssen and M. Ditzel, "Data Aggregation for Target Tracking in Wireless Sensor Networks", in Lecture Notes in Computer Science, vol. 4272, pp. 15-24, 2006.

[13] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", in IEEE/ACM Transactions on Networking, vol. 11, issue 1, pp. 2-16, February 2003.

[14] Mohamed Younis, Waleed Youssef, Mohamed Eltoweissy and Stephan Olario, "Safety-and-QoS Aware Management of Heterogeneous Sensor Networks", in Proceedings of the Eighth IEEE International Symposium on Parallel Architecture, Algorithms and Networks, pp. 386-391, 2005.
[15] Carlos F. Carcia-Hernandez, Pablo H. Ibarguengoytia-Gonzalez, Joaquin Garcia-Hermandez and Jesus A. Perez-Diaz, "Wireless Sensor Networks and Applications: A Survey", in International Journal of Computer Science and Network Security, vol. 7, pp. 264-273, March 2007.
[16] James Kay and Jeff Frolik, "Quality of Service Analysis and Control for Wireless Sensor Networks", in IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 359-368, October 2004.
[17] Richard J. Barton and Rong Zeng, "Order-Optimal Data Aggregation in Wireless Sensor Networks-Part I: Regular Networks", in IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 1-12, November 2007.
[18] Jie Gao, Leonidas Guibas and John Hershberger, "Sparse Data Aggregation in Sensor Networks", in Proceedings of The Sixth International Conference on Information Processing in Sensor Networks (IPSN07), pp. 430-439, April 2007.
[19] Gregory Hartl and Baochun Li, "Loss Inference in Wireless Sensor Networks Based on Data Aggregation", in Proceedings of The Third International Symposium on Information Processing in Sensor Networks (IPSN04), pp. 396-404, April 2004.

Shaila K is an Assistant Professor in the Department of Electronics and Communication Engineering at Vivekananda Institute of Technology, Bangalore, India. She received her B.E and M.E degrees in Electronics and Communication Engineering from Bangalore University, Bangalore. She is presently pursuing her Ph. D programme in the area of Wireless Sensor Networks in Bangalore University.

Nalini L obtained her Master of Computer Application from IGNO University. She is presently working in University Visvesv-araya College of Engineering.

Tejaswi V is a student of Computer Science and Engineering from Rastriya Vidayala College of Engineering, Bangalore. Her research interest is in the area of Wireless Sensor Networks.

Thriveni J is an Associate Professor with the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India. She received her B.E and M.E degrees in Computer Science and Engineering, from Bangalore University, Bangalore. She is obtained her Ph. D programme in the area of Wireless Adhoc Networks.

Venugopal K R is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph. D. in Economics from Bangalore University and Ph. D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 29 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has over 250 research papers to his credit. His research interests include Computer Networks, Parallel and Distributed Systems, Digital Signal Processing, Digital Circuits and Systems and Data Mining.

L M Patnaik is the Vice Chancellor, Defence Institute of Advanced Technology, Pune, India. He was a Professor from 1986 to 2008 in the Department of Computer Science and Automation, Indian Institute of Science, Bangalore. During the past 40 years of his service at the Institute he has over 700 research publications in refereed International Journals and Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to high Performance Computing and Soft Computing. His areas of research interest have been Parallel and Distributed Computing, Mobile Computing, CAD for VLSI circuits, Soft Computing and Computational Neuro-science.